UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN
AT LAW AND IN ADMIRALTY

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No.

APPROXIMATELY 10,983.26 TETHER (USDT) CRYPTOCURRENCY FROM BINANCE ACCOUNT USER ID NUMBER ENDING IN 6766,

Defendant.

VERIFIED COMPLAINT FOR CIVIL FORFEITURE IN REM

The United States of America, by its attorneys, Gregory J. Haanstad, United States Attorney for the Eastern District of Wisconsin, and Elizabeth M. Monfils, Assistant United States Attorney for this district, alleges the following in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

Nature of the Action

1. This is a civil action to forfeit property to the United States of America, under 18 U.S.C. §§ 981(a)(1)(A), 981(a)(1)(C) and 984, including cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1), for violations of 18 U.S.C. §§ 1343 and 1956.

The Defendant In Rem

2. The defendant, approximately 10,983.26 Tether (USDT) [1] cryptocurrency from Binance account user ID number ending in 6766, held in the name of Aqib Shaikh, was seized on or about March 21, 2024, in San Francisco, California.

[1] The value of Tether (USDT) is tied to the value of the United States dollar. Thus, the value of the defendant property is approximately $10,983.26.

3. The Federal Bureau of Investigation seized the defendant property pursuant to seizure warrant 24-M-366 issued by United States Magistrate Judge Stephen C. Dries in the Eastern District of Wisconsin on March 21, 2024.

4. The defendant property is presently in the custody of the Federal Bureau of Investigation in Milwaukee, Wisconsin.

Jurisdiction and Venue

5. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a).

6. This Court has *in rem* jurisdiction over the defendant property under 28 U.S.C. § 1355(b).

7. Venue is proper in this district under 28 U.S.C. § 1355(b)(1) because the acts or omissions giving rise to the forfeiture occurred, at least in part, in this district.

Basis for Forfeiture

8. The defendant, approximately 10,983.26 Tether (USDT) cryptocurrency from Binance account user ID number ending in 6766, is subject to forfeiture under 18 U.S.C. §§ 981(a)(1)(C) and 984 because it constitutes or was derived from proceeds traceable to an offense constituting "specified unlawful activity" – as defined in 18 U.S.C. § 1956(c)(7), with reference to 18 U.S.C. § 1961(1) – namely, wire fraud, committed in violation of 18 U.S.C. § 1343.

9. The defendant, approximately 10,983.26 Tether (USDT) cryptocurrency from Binance account user ID number ending in 6766, is also subject to forfeiture under 18 U.S.C. § 981(a)(1)(A) because it was involved in, or is traceable to funds involved in, money laundering transactions in violation of 18 U.S.C. §§ 1956 and 1957.

10. Section 1956 prohibits an individual from conducting or attempting to conduct "a financial transaction which in fact involves the proceeds of a specified unlawful activity knowing

that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of the specified unlawful activity."

11. Section 1957 prohibits an individual from engaging or attempting to engage in a "monetary transaction in criminally derived property of a value greater than $10,000 and is derived from a specified unlawful activity."

12. In any case in which the government seeks to forfeit property that either facilitated or was "involved in" the commission of the offense, the government must demonstrate a "substantial connection" between the property subject to forfeiture and the underlying criminal activity. 18 U.S.C. § 983(c)(3).

Facts

13. On March 4, 2024, an officer with the City of Oconomowoc Police Department ("OPD") met with a female victim identified as L.M. regarding a fraud complaint.

14. L.M. reported being the victim of a tech support fraud scam and having been defrauded a total of $23,800 as a result of the scam.

15. L.M. resides in the City of Oconomowoc, Waukesha County, which is located in the Eastern District of Wisconsin.

Details of the fraud scheme

16. On March 4, 2024, while paying bills online, L.M. received a pop-up alert on L.M.'s computer. The alert was purportedly from Microsoft Support and claimed that L.M.'s computer had been hacked. The alert instructed L.M. to call phone number (206) 388-2XXX for assistance.[2] L.M. called (206) 388-2XXX for assistance and spoke with a purported Microsoft Support employee ("purported MS employee"). The purported MS employee walked L.M.

[2] Based on publicly available information, area code 206 is associated with the Seattle, Washington area, where Microsoft has its headquarters.

through various steps to take on L.M.'s computer. During that call, the purported MS employee had remotely gained access to L.M.'s computer at a time when L.M.'s banking information was open on her computer.

A. Based on their training and experience, and the investigation to date, case agents believe that the purported MS employee obtained remote access to L.M.'s computer in an effort to gain information from L.M.'s computer.

B. OPD investigators observed approximately eight phone numbers that L.M. either called or received calls from on March 4, 2024. The phone numbers included: (206) 388-2XXX, (786) 864-4XXX, (800) 935-9XXX, and (866) 465-6XXX. These phone numbers return to Twillio, TextNow, Bandwidth, and other Voice Over Internet Protocol (VoIP) numbers.

C. Based on their training and experience, and the investigation to date, case agents are aware that Twillio, TextNow, Bandwidth, and other VoIP numbers are commonly used in fraud schemes to spoof legitimate businesses' phone numbers.

D. This type of fraud is commonly referred to as a "tech support scam." Microsoft Corporation warns users on their website to "protect yourself from tech support scams" with the following information:

> *Microsoft does not send unsolicited email messages or make unsolicited phone calls to request personal or financial information, or to provide technical support to fix your computer. If you didn't ask us to, we won't call you to offer support.*
>
> *If a pop-up or error message appears with a phone number, don't call the number. Error and warning messages from Microsoft never include a phone number.*
>
> *Microsoft will never ask that you pay for support in the form of cryptocurrency like Bitcoin, or gift cards.*

17. On March 4, 2024, L.M. also received calls from someone purporting to be with her bank – namely, from Chase Bank's Fraud Department ("purported CB employee"). The purported CB employee told L.M. that her bank account had been compromised.

18. The purported CB employee instructed L.M. to go to two different branches and withdraw a total of $23,800 in United States currency.[3] The purported CB employee further told L.M. that if bank personnel questioned L.M. when withdrawing the money, L.M. should tell them that it was money she needed for home repairs. The purported CB employee then instructed L.M. to deposit the $23,800 into a Byte Federal Bitcoin ATM located at Okauchee Wine, Beer & Liquor in Okauchee, Wisconsin.[4]

19. As instructed by the purported CB employee, L.M. withdrew a total of $23,800 from L.M.'s Chase Bank account in the following transactions:

A. On March 4, 2024, at approximately 11:50 a.m., L.M. withdrew $9,800 from L.M.'s account at a Chase Bank located in Oconomowoc, Wisconsin, and

B. On March 4, 2024, at approximately 2:31 p.m., L.M. withdrew $14,000 from L.M.'s account at a Chase Bank located in Delafield, Wisconsin.

20. As instructed by the purported CB employee, on March 4, 2024, L.M. deposited the $23,800 withdrawn from L.M.'s Chase Bank account into the Byte Federal Bitcoin ATM in Okauchee, Wisconsin ("Bitcoin ATM") by using the QR codes that the purported CB employee had texted to L.M. The four transactions totaling $23,800 at the Bitcoin ATM were as follows:

A. A deposit of $9,800 (ID: LPNCVRUKYY), which resulted in the purchase of, and conversion to, 0.1166250000 Bitcoin (BTC) cryptocurrency;

B. A deposit of $4,000 (ID: LY2G0EQIUP), which resulted in the purchase of, and conversion to, 0.0475879500 Bitcoin (BTC) cryptocurrency;

C. A deposit of $6,000 (ID: LACXB5VYRE), which resulted in the purchase of, and conversion to, 0.0712042300 Bitcoin (BTC) cryptocurrency; and

D. A deposit of $4,000 (ID: LXHKJYQXA9), which resulted in the purchase of, and conversion to, approximately 0.0474694800 Bitcoin (BTC) cryptocurrency.

[3] Based on their training and experience, case agents know that it is common for scammers to tell an account owner that they need to move their money "to keep it safe."

[4] Okauchee, Wisconsin is in Waukesha County, which is located in the Eastern District of Wisconsin.

21. On March 4, 2024, L.M.'s four deposits into the Bitcoin ATM totaling $23,800 in United States currency resulted in the purchase of, and conversion to, a total of approximately 0.28288666 Bitcoin, which Bitcoin were automatically transferred to the receiving Bitcoin wallet addresses per the QR codes provided to L.M. by the purported CB employee.

Tracing cryptocurrency from Bitcoin ATM

22. According to L.M.'s Byte Federal ATM transaction receipt and Binance records, on March 4, 2024, approximately 0.0474694800 Bitcoin (BTC) was purchased at the Bitcoin AMT for $4,000 in United States currency, was transferred from the Bitcoin ATM to Bitcoin address bc1qld94ew9hjmh5pquqvs56ujtgdaehsyystxpvge, and was then immediately transferred to address 1AxMcFEpVzpNYFhwbAGG5oVnCZENLcasmb (hereinafter referred to as "1AxM") via transaction hash c96b7eeac089318a7a8f6eb0b05c858c42aa669710e8eacb1c426986c508c98c (hereinafter referred to as "c96b7").

23. According to L.M.'s Byte Federal ATM transaction receipt and Binance records, on March 4, 2024, approximately 0.1166250000 Bitcoin (BTC) was purchased at the Bitcoin AMT for $9,800 in United States currency, was transferred from the Bitcoin ATM to Bitcoin address bc1qnqzvqrc7r37cr4wx3wus2mx35z8djh2pfgnrxr, and was then immediately transferred to the "1AxM" address via transaction hash eed32837413048661341feb300e028acf477aaa66b33fb2c4c8c732523915eab (hereinafter referred to as "eed32").

24. Based on analysis performed by law enforcement, the "1AxM" address is associated with the cryptocurrency exchange Binance.

Binance account user ID number ending in 6766

25. According to Binance records, the "1AxM" address is associated with Binance user account ID ending in 6766 ("Binance 6766") held in the name of Aqib Shaikh.

26. Binance 6766 was registered on or about March 31, 2022, using a Government of India identification card.

27. Binance records further show that on March 4, 2024, deposits were made into Binance 6766 of approximately 0.0474694800 Bitcoin (BTC) and approximately 0.1166250000 Bitcoin (BTC) using receiving address "1AxM" and transaction hashes c96b7 and eed32, respectively.

28. Binance records also show that on or about March 6, 2024, the account owner of Binance 6766 converted comingled funds of approximately 0.2341792 Bitcoin (BTC) to approximately 15,000 Tether (USDT).[5]

29. Based on analysis of the IP addresses used to access Binance 6766, the user's account was primarily accessed using IP addresses that geolocate to India. Based on the user's account information, as well as identity documents and access logs, case agents do not believe the account holder of Binance 6766 resides within the United States.

30. Based on their training and experience, and the investigation to date, case agents believe that the Binance 6766 account contained wire fraud proceeds. Additionally, the Binance 6766 account was involved in transactions designed, in whole or in part, to conceal or disguise the nature, the location, the source, the ownership, and the control of the approximately $23,800 stolen from L.M. in the fraud scheme.

[5] The value of Tether (USDT) is tied to the value of the United States dollar. Thus, the converted value was approximately $15,000.

31. Therefore, the defendant property, approximately 10,983.26 Tether (USDT) cryptocurrency from Binance account user ID number ending in 6766, constitutes wire fraud proceeds, in violation of 18 U.S.C. § 1343. The defendant property, approximately 10,983.26 Tether (USDT) cryptocurrency from Binance account user ID number ending in 6766, was also involved in money laundering, in violation of 18 U.S.C. §§ 1956 and 1957.

Warrant for Arrest In Rem

32. Upon the filing of this complaint, the plaintiff requests that the Court issue an arrest warrant *in rem* pursuant to Supplemental Rule G(3)(b), which the plaintiff will execute upon the defendant property pursuant to 28 U.S.C. § 1355(d) and Supplemental Rule G(3)(c).

Claim for Relief

33. The plaintiff repeats and incorporates by reference the paragraphs above.

34. By the foregoing and other acts, the defendant property constitutes or was derived from proceeds traceable to specified unlawful activity, namely, wire fraud, committed in violation of 18 U.S.C. § 1343, and is therefore subject to forfeiture to the United States of America under 18 U.S.C. §§ 981(a)(1)(C) and 984, with cross-references to 18 U.S.C. §§ 1956(c)(7) and 1961(1).

35. By the foregoing and other acts, the defendant property was involved in, or is traceable to funds involved in, money laundering transactions in violation of 18 U.S.C. §§ 1956 and 1957, and is therefore subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(A).

WHEREFORE, the United States of America prays that a warrant of arrest for the defendant property be issued; that due notice be given to all interested parties to appear and show cause why the forfeiture should not be decreed; that judgment declare the defendant property to be condemned and forfeited to the United States of America for disposition according to law; and that

the United States of America be granted such other and further relief as this Court may deem just and equitable, together with the costs and disbursements of this action.

Dated at Milwaukee, Wisconsin, this 7th day of August, 2024.

Respectfully submitted,

GREGORY J. HAANSTAD
United States Attorney

By: *s/Elizabeth M. Monfils*
ELIZABETH M. MONFILS
Assistant United States Attorney
Wisconsin Bar No. 1061622
Office of the United States Attorney
Eastern District of Wisconsin
517 E. Wisconsin Avenue, Room 530
Milwaukee, WI 53202
Telephone: (414) 297-1700
Fax: (414) 297-1738
E-Mail: elizabeth.monfils@usdoj.gov

Verification

I, Ashley Gentle, hereby verify and declare under penalty of perjury that I am Special Agent with the Federal Bureau of Investigation ("FBI"), that I have read the foregoing Verified Complaint for Civil Forfeiture *in rem* and know the contents thereof, and that the factual matters contained in paragraphs 13 through 31 of the Verified Complaint are true to my own knowledge.

The sources of my knowledge are the official files and records of the United States, information supplied to me by other law enforcement officers, as well as my investigation of this case, together with others, as a Special Agent with FBI.

I hereby verify and declare under penalty of perjury that the foregoing is true and correct.

Date: 08/06/2024

s/Ashley Gentle
Ashley Gentle
Special Agent
Federal Bureau of Investigation